A Power Management System

ALI CHRAKIE, MOUSTAPHA EL HASSAN, JIHAD DABA
Department of Electrical Engineering,
University of Balamand,
Koura,
LEBANON

Abstract: - This paper addresses the need for a dependable, safe, and user-friendly power management solution. This system transforms electricity distribution by emphasizing advanced user subscription management, cost-effective distribution techniques, and intelligent theft detection. Key features include power theft detection, over-limit current detection, email alerts for users and administrators, a website for administrators to monitor the system, an app for users to track their home status, and a control server for managing user's current limits and subscription statuses. Additionally, the system's cost-effectiveness adds significant value compared to existing prototypes. The study includes examining the current state of power management, evaluating the benefits and limitations of various existing systems, and providing comparative analysis to determine the optimal design approach. The research outcome is a design that prioritizes Sustainability, efficiency, and security. Additionally, we have simulated, implemented, and tested a prototype, and the results validate the design.

Key-Words: - Power management system, Power theft detection, Real-time monitoring, Smart meters, Current limit control, Energy distribution, IoT integration, Over-limit detection, Energy efficiency, Sustainability.

Received: May 29, 2024. Revised: November 18, 2024. Accepted: December 23, 2024. Published: April 9, 2025.

1 Introduction

Never has there been such a crucial need for a reliable and secure power management system in energy distribution and usage. This work presents an improved power distribution, monitoring, and security approach. Our interest in this topic stems from the persistent challenges of power theft detection and prevention, which cause significant financial losses to utilities and disrupt fair usage among consumers. It foresees the development of a power management system incorporating advanced technology in power theft detection. The integration of advanced power theft detection technology offers a seamless and cost-effective way to distribute electricity with consideration of customer subscriptions. Its exceptional strength is its capability to prevent power theft and speedy alert systems for administrators and users about unauthorized connections.

The method developed through this research is flexible and easy to integrate into different buildings and utilities. The technology reduces operational risks and disruptions since it can allow real-time user limit changes and subscription activation/cancellation through a control server. The system also provides a website for administrators to monitor user parameters and an application for users to monitor their houses and control their consumption.

These results confirm that this power management system could significantly reduce theft and increase operational efficiency toward a more sustainable and safer future. The paper discusses various fields by reviewing recent research and prototypes and comparing their unique characteristics. The work will include a discussion of the planning, execution, and results of the study by presenting a comprehensive analysis, calculations, and prototype development. A testing evaluation of this prototype will be given, together with its benefits and possible directions for innovation and further improvement.

2 Literature Review on Existing Power Theft Detection Systems

Energy theft has been one of the significant drawbacks of power distribution networks. Thus, several creative solutions have developed. Several works stressed the importance of detecting illegal electricity usage for energy-tracking systems. In paper [1], the security enhancement is based on a

PIC Microcontroller that cooperates with peripherals like a GSM modem, voltage regulator, bridge rectifier, and MAX 232 for communication and power monitoring for wireless data transmission and real-time theft detection. Similarly, the SMS-based automatic meter reading system described in [2] uses GSM to help enhance operating efficiency and nip thefts.

Some research on electricity theft detection has used radio frequency-based applications, showing the promising role of wireless communication technologies in this. In [3], Arduino technology helps continuously monitor the current flow passing through any line. It transmits data wirelessly, with help from various hardware components like a Hall Effect sensor and a 433 MHz module. Research in [4] reveals that components like a Hall Effect sensor and a 433 MHz module enable wireless theft detection via Zigbee technology, secure real-time monitoring, and active data transmission to the utility.

On the other hand, different works have reduced power theft using various methods. In [5], technical and nontechnical losses are handled by using Arduino microcontrollers and step-down transformers with cloud-based communication to monitor it in real time and the detection of theft. It also covers prepaid credit controls and power cutoffs. Similarly, abnormal consumption patterns in power usage have been dealt with in [6] regarding local-level theft detection and control.

Other works, such as in [7] and [8], researched how well IoT and techniques from data mining may put forth their case to assist energy theft detection. Particularly in [7], it proposes an architecture using sensors that communicate with a Microcontroller over GSM and immediately give indications of theft incidents upon occurrences. Its companion work [8] explains how various data mining methods are employed to enhance the efficiency of theft detection for residential customers, speeding up responses to energy changes.

Various research has pointed out the use of GSM technology to enhance the detection of power theft [9], [10]. In [9], the proposed system is based on a PIC Microcontroller using CT sensors for energy flow tracking and GSM to send theft intimation to the utility board. The presented system contains a bridge rectifier and voltage regulators that ensure stable operation. In this regard, [10] also proposes a GSM-based theft detection system that is possible to apply in both residential and commercial settings, stressing the role of modern communication technologies in making the process of detection and reporting easier.

Studies [11] and [12] introduce other advances in fighting electricity theft, focusing on dual-meter and advanced systems. In [11], the authors propose a system with a dual-energy meter, using GSM and Bluetooth, to monitor energy consumption differences at distribution and consumer levels. The technique promises fast detection and notification to utilities. Finally, [12] refers to more general anti-theft measures in Nigeria, describing technological interventions impacting revenue assurance and lower electricity theft.

In [13] and [14], the focus was on systems for detecting unauthorized electricity use based on GSM. The system described in [13] utilizes a PIC Microcontroller and current transformers to monitor power discrepancies and send real-time SMS to utilities. Similarly, in [14], a GSM-based automatic meter reading system that applies telecommunication technologies to improve theft control and utility management is presented.

Works in [15] and [16] introduce new systems based on modern IoT and Arduino technologies for detecting power theft. [15] proposes a system for measuring power discrepancies with current and voltage transformers, sending warnings via IoT MQTT applications. In turn, [16] proposes IoT-based solutions to automate detecting theft, which will give quick and accurate responses.

The studies [17] and [18] represent state-of-the-art IoT and GSM monitoring and theft detection systems. The IoT-based system proposed by researchers in [17] allows real-time power consumption monitoring using Raspberry Pi and Arduino, sending an alert to utilities through GSM if it detects theft. On similar lines, the author in [18] explains a wireless approach in power monitoring based on using GSM to report theft, making timely actions possible.

Several works have been conducted on GSM-based systems to enhance communication efficiency and detect theft cases, [19], [20]. Based on this concept, for remote control at power access, a power monitoring system based on a GSM real-time theft utility communication is proposed in [19]. In [20], the authors propose another energy meter with a GSM basis that simplifies the process of energy monitoring and theft detection, enhancing security and management in utilities.

The studies [21] and [22] provide more general solutions to utility theft, including exploring the role of IoT in urban infrastructure. In [21], the authors investigate how smart meters and cloud-based data analytics make possible the automation of theft detection and enhancement of resource distribution. Moreover, [22] provides a comparative analysis of the economic impact of electricity theft, emphasizing the need for advanced technologies to protect and manage resources.

This research utilizes Microcontrollers PIC and Arduino, GSM modules, current transformers, and cloud-based IoT integration to prevent energy theft. Most of the research concentrates on real-time notification for theft detection based on GSM, [1], [9]. This approach, using IoT and data mining for dynamic monitoring, was expanded in [7] and [8]. Some of the promising wireless technologies being used to detect theft include GSM [13], [14] and Zigbee, [4]. Smart meters, cloud-based analytics, and dual-energy metering are key components of advanced systems that provide scalable real-time monitoring. These works emphasize integrating secure hardware with state-of-the-art communication and data analysis technologies to develop effective and secure theft detection systems.

3 Proposed Power Theft Detection and Management System

The research team developed a comprehensive solution that builds on various power theft detection systems by integrating key technologies and methodologies from these studies. Our system incorporates wireless data transmission inspired by [1] and Arduino-based monitoring findings, as seen in [3], where current sensors and microcontrollers track energy consumption. Like the approach in [5], our system employs real time cloud-based monitoring. It features a relay system that automatically cuts off power when theft or over-limit conditions are detected, ensuring an immediate response. As highlighted in [17], the IoT-based design framework facilitates seamless data transmission and real-time updates for users and power companies.

Our system, built on these foundations, measures additional parameters such as voltage, frequency, current, and power factor, similar to the advanced systems reviewed. These parameters enable the system to calculate real-time power consumption and log energy usage over time, effectively functioning as an energy meter. At the heart of the system is the Arduino Mega 2560, integrated with ESP32 modules for wireless data communication, which ensures accurate detection of discrepancies between household and mainline currents to identify power theft. Drawing from cloud-based monitoring techniques in the systems discussed in [5] and [19], our system continuously updates a ThingSpeak-based monitoring website. It utilizes a separate control server to execute commands and cut off power when necessary.

Our system further introduces remote management capabilities through the control server, enabling power companies to adjust user settings, set current limits, and manage subscription cancellations, a feature inspired by systems like [9]. Additionally, the system sends email notifications to users and administrators in cases of over-limit or theft detection, allowing for temporary or permanent power cutoffs based on the situation. Like the approach in [11], our system includes a user-friendly app for real-time monitoring, allowing users to track their energy consumption and make informed decisions to optimize their usage.

Our system represents a novel, culminating design that synthesizes the strengths of various power theft detection systems grounded in extensive research. We have carefully analyzed the advantages of different designs and methodologies, incorporating the best features from each. While many existing systems excel in specific areas, none have successfully combined all the critical features into a single comprehensive solution. Our system integrates these diverse technologies and improves upon them by selecting and refining the most effective approaches. Our robust, scalable, and cost-effective energy management system, designed to detect power theft and enhance energy logging, real-time monitoring, remote control, and automated actions, uniquely addresses modern energy management challenges in ways existing designs do not.

Figure 1 illustrates the design block diagram detailing each component's interconnections and flow mechanisms. It provides a comprehensive overview of how each block interacts within the system, demonstrating the sequential processes and data flow that drive overall functionality. The Arduino Mega 2560 Rev 3 is at the center, which manages most processed parameters. Below the Arduino is the ESP32, which receives data wirelessly from other ESP32 modules at each home. The ESP32 transmits this data to the Arduino for processing. The current sensor, ACS712, positioned above the ESP32 on the right side, measures the wirelessly transmitted data, which is computed and sent for further processing. Once the Arduino processes the data, it measures the difference between the current reading at each home (transmitted wirelessly) and the current sensor reading on the main line. The difference between the current readings from the sensor at the user side and the primary sensor at the distribution line should not exceed 5%. This comparison is conducted across multiple samples within a 10-second to determine if power theft has occurred. Arduino then sends the data back to ESP32 above Arduino, which is responsible for transmitting the information to Thing-Speak Cloud for the monitoring system. This ESP32 also updates the control server, executes commands, and generates emails, effectively playing a controlling role. To the left of the Arduino is the 12V power supply, which powers the MCUs. To the Arduino's right is a relay for each home. If theft is detected or consumption exceeds the limit, the ESP32 controls the relay by sending a signal (0 or 1) to cut off or restore power accordingly.

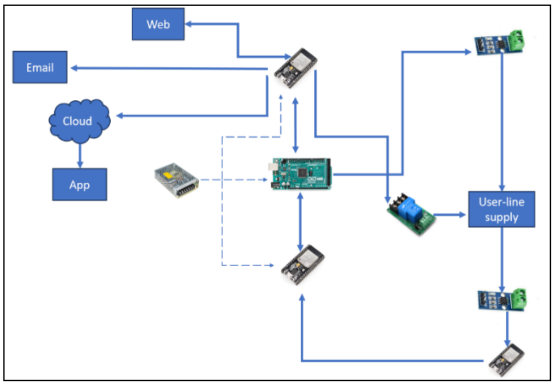


Fig. 1: Design Block Diagram

We used a stepped-down rectified signal with positive peaks within the suitable range for the Arduino. By sampling this signal, we measured the input voltage and frequency. We determined the source voltage by considering diode losses of 1.4V and using the known turns ratio of 53.

Figure 2 shows a sine wave with a peak of 3.13V, which the Arduino will sample using an analog pin. The ACS712 sensor produces a sine wave centered at 2.5V, alternating above and below this value. In this measurement, the peak voltage increases by 66mV for each 1A increase in load, allowing for precise monitoring of changes in current through the system. In this case, a 3.13V measurement corresponds to a 0.63V increase in the sensor output (3.13V - 2.5V = 0.63V). By performing the calculations, 0.63V / 0.066 = 9.54A, so the load corresponds to a 9.54A current.

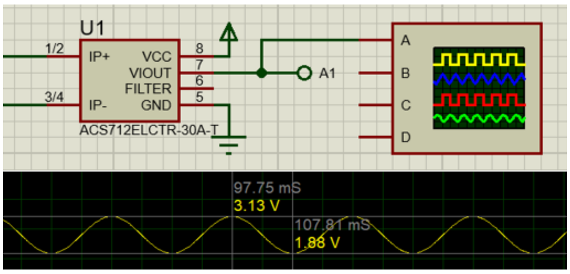


Fig. 2: Measuring Current Using ACS712

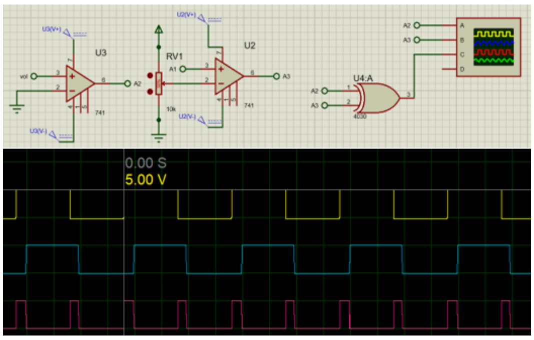


Fig. 3: XOR Gate Logic Power Factor Measurement

Figure 3 illustrates three clock signals: the 741 op-amps generate the top and middle signals, while the XOR gate produces the bottom by processing the top and middle clock signals as inputs. The top waveform represents voltage, the middle waveform represents current, and the bottom waveform represents the power factor measurement, which operates with a variable duty cycle determined by the power factor. XOR logic determines the phase relationship between the voltage and current waves. When both are in phase (both zero or both 1), the XOR output is 0. If out of phase, the XOR output rises to logic 1 for a particular duration. This duration is measured and applied to equations 1, 2, and 3 to calculate the power factor. The bottom clock signal is generated only for visual illustration, with the XOR logic implemented directly in the Arduino to reduce the need for additional components. The Arduino will also detect whether the current leads or lags the voltage.

To calculate the period of the electrical signal, we used the previously measured frequency, as outlined in (1). Based on this period and the time difference shown in Figure 3, we determined the phase angle using equation (2). With this angle, we compute the power factor using (3), enabling accurate calculations, as shown in (4). After determining the real power, we calculate the total energy consumed as presented in (5), effectively linking power consumption over a specified period to energy usage.

$$Period = \frac{1}{Frequency} \tag{1}$$

$$Angle = \frac{360 * Time\ Difference}{Period} \tag{2}$$

$$Power\ Factor = \cos(Angle) \tag{3}$$

$$P = V * I * Power\ Factor \tag{4}$$

$$E = P * T \tag{5}$$

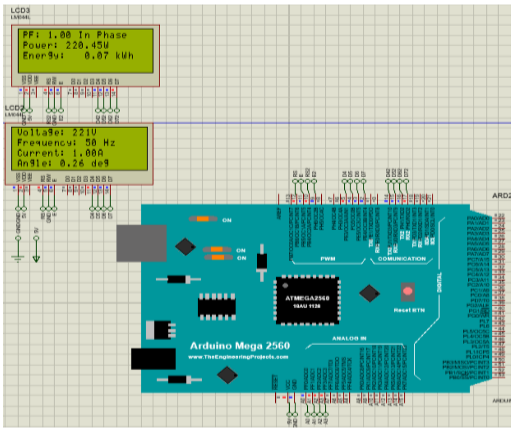


Fig. 4: Resistive Load Simulation

Figure 4 illustrates the results of testing a resistive load, where a current of 1A and a voltage of 221V were applied. The power factor was computed as 1, yielding a power usage of 220.45W, consistent with the expected value. In Figure 5, the experimental setup included the addition of an inductive load to the resistive load, resulting in a current of 1.23A and a voltage of 221V. The calculated power factor was 0.83 lagging, and the researchers determined the power usage to be 220.40W, closely aligning with the real power of 220.45W measured in Figure 4. The resistance remained constant, affirming that the real power should not change. The 0.05W discrepancy between these values is negligible, attributed to standard decimal variations common in practical measurements. This finding underscores the reliability and accuracy of the power factor and related parameters in both scenarios.

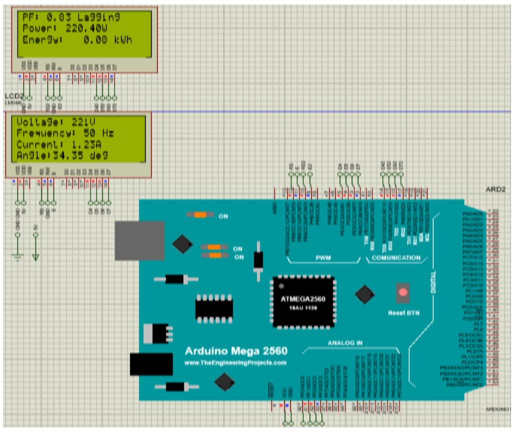


Fig. 5: Inductive Load Simulation

In Figure 6, the inductive load was substituted with a capacitive load while maintaining the same resistance. This setup produced a current of 1.21A and a power factor of 0.84 leading. The computed power usage was 220.59W, which aligns closely with the previous measurements of 220.45W and 220.40W. Since the resistive load remained unaltered, these results validate the consistency and reliability of the power factor measurement methodology.

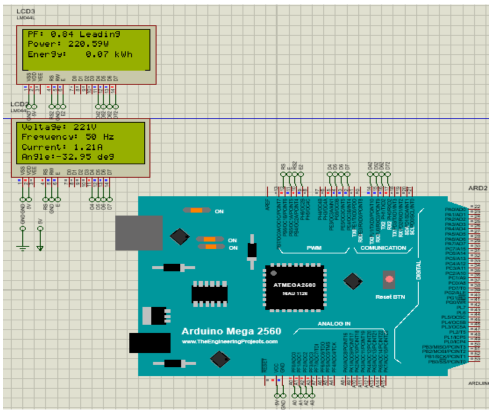


Fig. 6: Capacitive Load Simulation

4 Implementation and Results

Figure 7 shows the built prototype for detecting power theft, which follows the design block diagram and working procedure outlined in Figure 1. The prototype includes an Arduino Mega 2560 Rev 3, current sensors, relays, and ESP32 units, all working together to measure, transmit, and process data.

To verify the performance of each block, we conducted tests. In Figure 8, the voltage measurement test (top left) showed a reading of 216V from the meter, while the Arduino recorded it as 217V. This difference falls within a range of less than 1% error. This close correspondence confirms the accuracy of the voltage measurement block. On the bottom left of Figure 8, the meter recorded a frequency of around 50 Hz during the frequency measurement test. At the same time, the Arduino measured it precisely at 50Hz, affirming the functionality of the frequency measurement block.

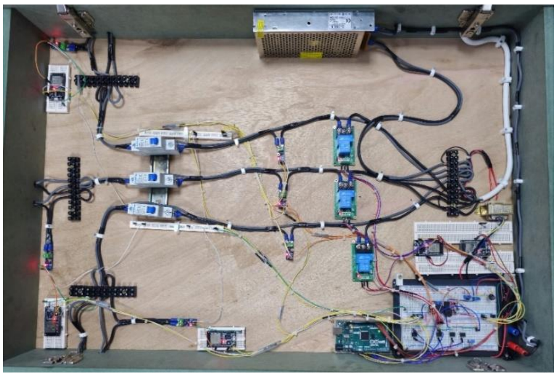
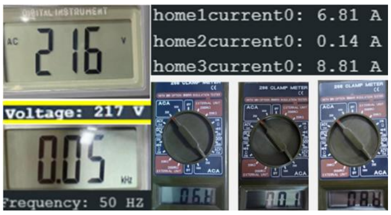


Fig. 7: Implemented Prototype

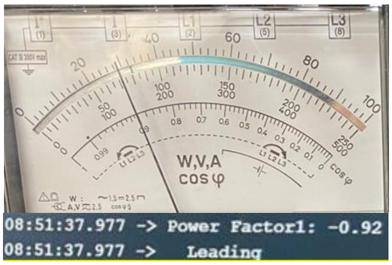
On the right side of Figure 8, we measured three currents, one for each user, and compared them with the meter readings. For User 1, the meter recorded a current of 6.8A, while the Arduino measured it as 6.81A. For User 2, the meter reading was 0.1A, while the Arduino recorded it as 0.14A. Finally, for User 3, the meter displayed a current of 8.8A, and the Arduino measured it as 8.81A. These close correspondences between the meter and Arduino measurements validate the effectiveness of the current measurement block. The system records measurements with two decimal places, while the meter records only one, offering higher accuracy. The first decimal recorded by the system consistently matches the meter's reading, resulting in an error of less than 1%.



```
home1current0: 6.81 A
home2current0: 0.14 A
home3current0: 8.81 A
Voltage: 217 V
Frequency: 50 HZ
```

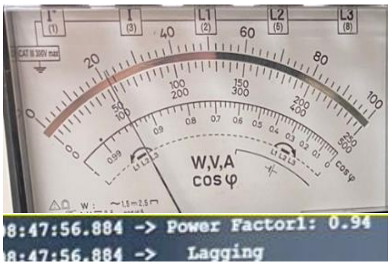
Fig. 8: Voltage, Frequency, and Home Currents Measurement

We tested the power factor measurement for both lagging and leading conditions. In Figure 9(a), the meter recorded a power factor of 0.94 Lagging, which the Arduino also measured precisely as 0.94 Lagging, confirming the effectiveness of the power factor measurement. In Figure 9(b), the meter displayed a power factor of 0.91 Leading, while the Arduino measured it as 0.92 Leading. This close agreement between the meter and Arduino measurements, with an error of less than 1%, demonstrates the accuracy of the power factor measurement.



```
08:51:37.977 -> Power Factor1: -0.92
08:51:37.977 ->   Leading
```

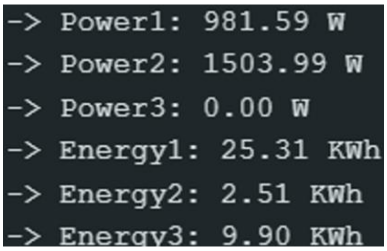
Fig. 9 (a): Leading Power Factor Measurement



```
8:47:56.884 -> Power Factor1: 0.94
8:47:56.884 ->   Lagging
```

Fig. 9 (b): Lagging Power Factor Measurement

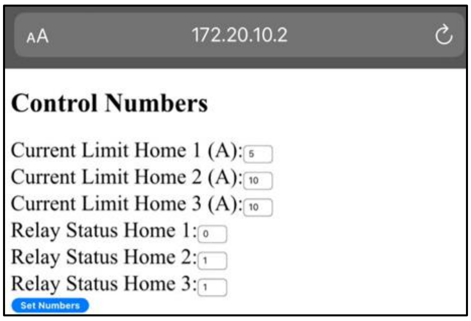
Given that we are measuring voltage, frequency, current, and power factor, we can calculate the actual power used (4). Furthermore, with the power obtained from (5), we can determine the energy consumed over time. We can achieve this functionality by setting a time interval using the Arduino. These power and energy measurements are conducted for each user, as shown in Figure 10. As discussed, all measurements, such as voltage, frequency, current, and power factor, fall within an error range below 1%. Therefore, we can ensure that the obtained results are precise.



```
-> Power1: 981.59 W
-> Power2: 1503.99 W
-> Power3: 0.00 W
-> Energy1: 25.31 KWh
-> Energy2: 2.51 KWh
-> Energy3: 9.90 KWh
```

Fig. 10: Power and Energy Used by Each User

Figure 11 illustrates the Control Server, the central hub for controlling user subscriptions and current limits. This interface allows administrators to modify these values as required quickly. Notably, a value of 0 indicates that the system has cut off power, while a value of 1 signifies that power is accessible. Only the administrator, using a username and password, can access the control server, ensuring safety and security.



Control Numbers

Current Limit Home 1 (A): 5
Current Limit Home 2 (A): 10
Current Limit Home 3 (A): 10
Relay Status Home 1: 0
Relay Status Home 2: 1
Relay Status Home 3: 1

Fig. 11: Control Server

Figure 12 shows the relay status. The correct relay's LED flashes red to indicate a power cutoff. The system assigns the proper relay to Home 1, the middle relay to Home 2, and the left to Home 3. A red LED signals that the system has cut off power, while a non-flashing LED shows power availability. If a user exceeds the current limit, the relay cuts off power as commanded by the ESP32 MCU, and the system restores power after one minute. In the case of power theft, the ESP32 MCU issues a permanent cutoff command until the administrator restores access after investigating the issue. During this time, the red LED flashes until the system restores power.

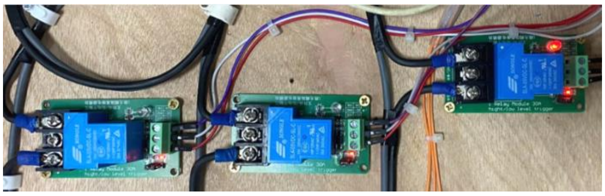
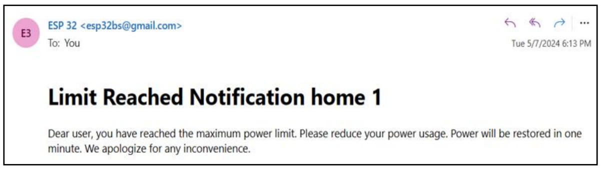


Fig. 12: Power Cutoff for Home 1

The system operates under various scenarios where users can control each relay independently. For example, an over-limit detection may occur in Home 3, resulting in a one-minute power cutoff. In contrast, Home 2 retains power access, and Home 1 experiences a permanent power cutoff due to power theft detection. Alternatively, users can configure the system so that all homes have their power permanently cut off due to theft detection in each home, or Home 1 and Home 3 could experience temporary power cutoffs due to over-limit detection. In contrast, Home 2 continues to have power access. The prototype uses an Arduino Mega 2560 Rev3 Microcontroller and currently supports three users. Users can expand the system to support up to 10 users by adding more sensors and relays. If the system supports more than 10 users, it will require a Microcontroller with more GPIOs than the Arduino Mega, as it heavily depends on ADC pins. For a more extensive implementation involving 30, 40, or more users, we will need a Microcontroller with more significant memory and computational speed to ensure the system's speed and reliability. The design accommodates as many users as required, depending on the Microcontroller's capabilities.

Figure 13 shows an email sent to the user, informing them that the system has reached the power limit for Home 1 and will restore power in one minute. This proactive communication informs users of disruptions and reassures them of a swift resolution. In this scenario, the correct relay corresponding to Home 1, as shown in Figure 12, cuts off the power. We can apply the same scenario to Homes 2 and 3.



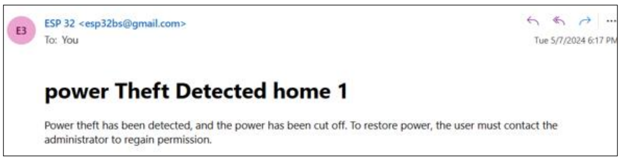
E3 ESP 32 <esp32bs@gmail.com>
To: You
Tue 5/7/2024 6:13 PM

Limit Reached Notification home 1

Dear user, you have reached the maximum power limit. Please reduce your power usage. Power will be restored in one minute. We apologize for any inconvenience.

Fig. 13: Email Alert Message for Reaching Limit

In the second scenario, we simulated an illegal load bypassing the meter, specifically testing it on Home 1. Figure 14 shows an email alert notifying the user that the system detected power theft, resulting in a power cutoff. The system instructs the user to contact the administrator to regain power access. This proactive measure ensures that the system promptly addresses unauthorized activities, preventing further misuse of resources. The relay on the right, responsible for Home 1, as shown in Figure 12, will flash red and cut off power. We can similarly apply this scenario to Homes 2 and 3, with the respective relays responding similarly.



E3 ESP 32 <esp32bs@gmail.com>
To: You
Tue 5/7/2024 6:17 PM

power Theft Detected home 1

Power theft has been detected, and the power has been cut off. To restore power, the user must contact the administrator to regain permission.

Fig. 14: Email Alert Message for Detecting a Theft

Similarly, we tested a power theft scenario on Home 3. As shown in Figure 15, the left relay for Home 3 was flashing red, indicating a power cutoff. Previously, power theft was detected in Home 1, causing the correct relay for Home 1 to flash red and resulting in a permanent power cutoff for Home 1. After detecting power theft in Home 3, both Home 1 and Home 3 experienced permanent power cutoffs, while Home 2 continued to have power access.

Additionally, we tested a power theft scenario on Home 2, where there was a power cutoff due to previous power theft detection in Homes 1 and 3. After detecting power theft in Home 2, a power cutoff was triggered for all three homes. As shown in Figure 16, the red LEDs on all relays are flashing, indicating a power cutoff for Homes 1, 2, and 3.

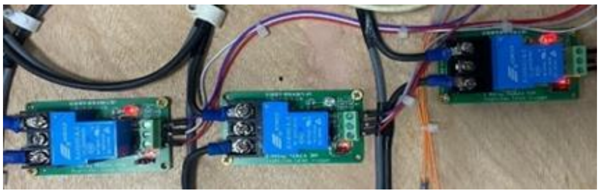


Fig. 15: Power Cutoff for Home 1 and 3

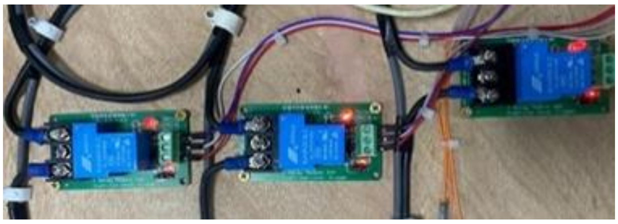


Fig. 16: Power Cutoff for Homes 1, 2 and 3

The power theft and over-limit detection scenarios apply to all users, including Homes 1, 2, and 3, and additional users if the system expands.

With this Microcontroller, the system can support up to 10 users. These scenarios validate the effectiveness of the design, confirming that the system functions as intended.

Figure 17 shows the measured voltage for Home 1, an online monitoring website developed using Thing-Speak displays. The measured voltage fluctuates around 220V, which is the nominal input voltage.

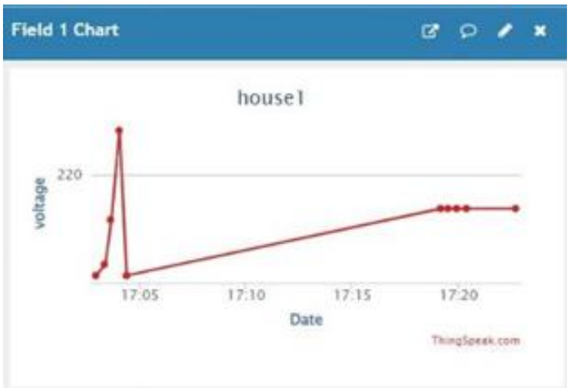


Fig. 17: Company Server for Monitoring Measured Voltage

Figure 18 shows the measured current at Home 1. The current variation reflects when the home is loaded or unloaded, with the monitor updating the server directly. In this scenario, the current was around 7A.

Figure 19 shows the measured frequency, displaying a constant value of 49 Hz, close to the nominal input frequency of 50 Hz. The system expects a continuous display, as the frequency should remain stable.

Figure 20 shows the power consumed, which displays a similar pattern to the current, as the system calculates the power using Equation 4. In this scenario, the power was around 1.5 kW.

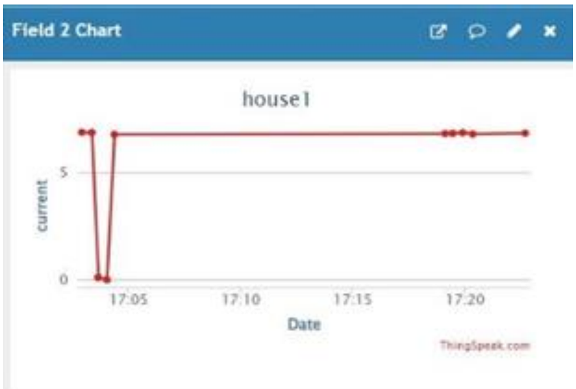


Fig. 18: Company Server for Monitoring Measured Current

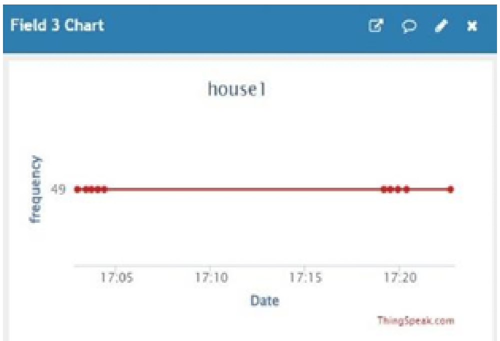


Fig. 19: Company Server for Monitoring Measured Frequency

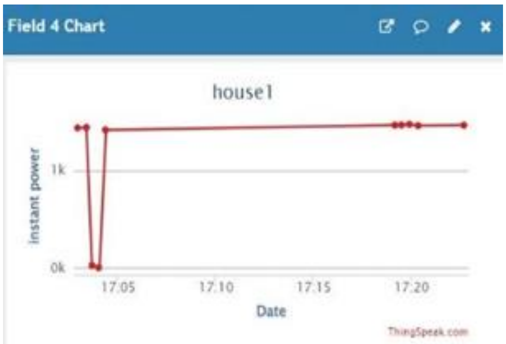


Fig. 20: Company Server for Monitoring Measured Instant Power

Figure 21 shows the total energy consumed, a meter that continuously increases over time. Since the system records the energy for tracking consumption, it functions like a traditional energy meter.

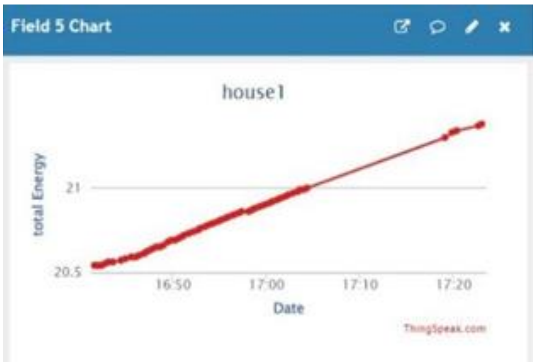


Fig. 21: Company Server for Monitoring Measured Energy

Figure 22 shows the power factor, which varies between -1 and 1. The power factor ranges between 0 and 1 for an inductive load, while it ranges between 0 and -1 for a capacitive load. This variation helps track low power factors, allowing the system to alert the user if the power factor drops significantly.

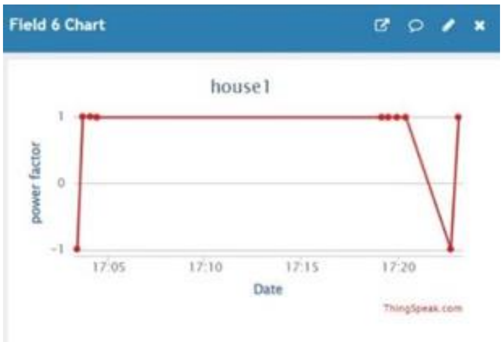
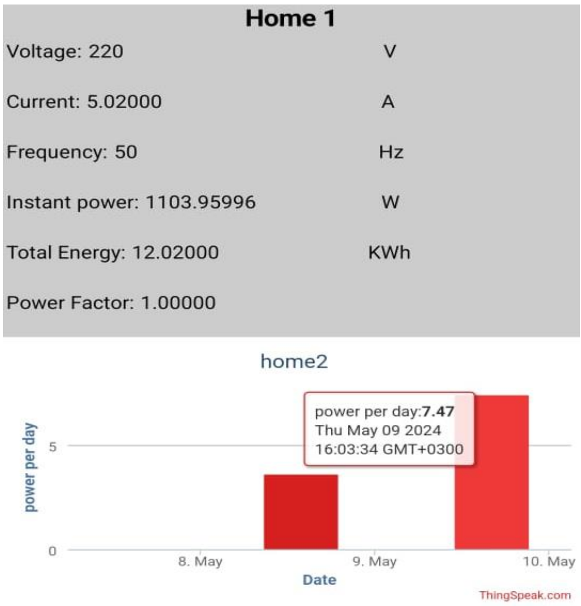


Fig. 22: Company Server for Monitoring Measured Power Factor



Home 1

Voltage: 220	V
Current: 5.02000	A
Frequency: 50	Hz
Instant power: 1103.95996	W
Total Energy: 12.02000	KWh
Power Factor: 1.00000	

Fig. 23: App for User Monitoring for the Measured Parameters

We have designed an application that gives users access to their home status and a summary of power consumption. Figure 23 introduces the application, which comprehensively displays essential parameters such as voltage, frequency, current, and power factor. Additionally, it provides details on instantaneous power usage, cumulative energy meter records, and daily energy consumption statistics. This user-centric interface equips individuals with the tools to monitor and manage their power utilization efficiently. For example, it shows energy usage of 7.47 kWh per day, as illustrated in Figure 23. Figure 23 displays the report for Home 1, with similar displays available and accessible for Homes 2 and 3 users.

5 Cost

Comparing leading market models like the XENIUS and RISESUN smart meters reveals key differences. The XENIUS Smart Energy Meter, priced at $258, offers theft detection and essential electrical parameters but lacks live monitoring and real-time user interaction. The AMI Smart Meter, costing $150, provides similar features but is more cost-effective. In contrast, this research emphasizes comprehensive real-time data feedback, future scalability for home automation, and a cost-effective solution that adds significant value beyond existing prototypes.

The proposed system, designed with accurate and reliable low-cost components, measures all electrical parameters and detects power theft and over-limit conditions. It controls the current limit and user subscription status through a control server, allowing the administrator to monitor the status of each home via a website. Additionally, a user application enables homeowners to monitor their home status. The system will restore power in a minute and automatically generate emails for users and administrators when it detects an over-limit condition or theft.

This design is notably cheaper than the existing options. For a single user, it costs $110.83—less than the least expensive existing option. For multiple users, costs are even more efficient: $145.53 for three users and $266.98 for ten, resulting in a price per user of about $26.69, making it 562% cheaper than the cheapest existing option. The system's low cost and extensive features make it an attractive solution that can be further enhanced by adding more features based on demand.

6 Sustainability

Its design includes sustainable features, as seen in Figure 7, due to using a compact single-box unit that is approximately 1.5 meters high and 1 meter wide. This box can replace traditional circuit breakers and energy meters and provide the same functions and added functionality. The design is compact compared to conventional energy meters since it consolidates all tasks into a smaller unit.

Another key system component is power theft detection, which helps reduce power wastage and overall power consumption. Through the user monitoring app, the user will also be able to manage their energy consumption based on accurate data. The design capability to measure power factors allows for detecting low power factors. In some instances, poor performance regarding the power factor may trigger an alert for the customers from the power company for remedial measures or the application of penalties and extra fees. Besides, the design increases overall efficiency by saving additional components.

7 Conclusion

The target of this research work is a practical implementation of the "Power Management System" that is facing serious problems of energy distribution inefficiencies and electricity theft. Incorporating sophisticated technology such as the IoT allows real-time monitoring for theft of electric current, detecting over-limit currents, subscription management at consumer levels, etc. The system precisely measures and monitors vital electrical variables such as voltage, frequency, current, power factor, power consumption, and energy usage. The system has a control server for real-time changes and an administrator website for monitoring. It also has a user-friendly application that allows home occupants to manage their power usage and monitor consumption easily.

The main objective of this study was to develop a system that provides a scalable and economical energy distribution solution in addition to detecting power theft. We ensured that users and administrators could communicate easily by integrating alarm systems and dynamic control elements. Since we simulated the system, constructed a functional prototype, and thoroughly tested it, our design has effectively complied with these specifications. The prototype produced the anticipated outcomes, demonstrating that the system functions as planned and can respond quickly to anomalies such as power theft. This technology makes a more secure and sustainable electricity distribution system possible, which provides a strong basis for upcoming upgrades and additional operational efficiency gains.

8 Future Work

Significant extensions are planned for future work to improve the operational efficiency and resilience of our "A Power Management System," which presently focuses on power theft detection and management. One significant advancement will be the incorporation of cutting-edge Automatic Power Factor Correction (APFC) technologies. As noted by [23], this involves installing an automatic power factor detection and correction system that uses a microprocessor with capacitor banks to keep the power factor around unity and deal with inductive load inefficiencies. Several writers have demonstrated that we can use Arduino microcontrollers [24], [25] and [26] to make dynamic power factor modifications for both home and commercial settings.

Additionally, incorporating IoT-enabled APFC systems can improve flexibility and reduce human intervention, increasing overall stability and energy efficiency. Furthermore, as suggested by [27] and [28], sophisticated APFC algorithms that use cross-coherence coefficients between voltage and current signals and real-time Pearson correlation coefficients for dynamic changes can be added, improving efficiency and stability. As an alternative, reliable hardware solutions can guarantee quick reactive power adjustments, such as the Arduino-based system [29] and the thyristor-based APFC unit, [30]. Finally, stressed by [31] and shown by [32], it will be critical to use the cost-saving potential of APFC technology to lower capital investment and avoid equipment damage.

Future studies will concentrate on incorporating Automatic Power Factor Correction (APFC) into the "A Power Management System," which presently handles power theft detection and management. These enhancements in the 'A Power Management System' will build on the fundamental research examined in the literature on Automatic Power Factor Correction (APFC). By dynamically modifying power factors in real-time, increasing electrical load efficiency, and lowering transmission losses, the system seeks to use the most recent developments in APFC technology to maximize effectiveness.

Since our "A Power Management System" uses Arduino microcontrollers, the most appropriate strategy is the one described by [24], [25] and [30], who used Arduino-based APFC solutions, even if the other APFC implementation techniques examined in this study might work with our system. In addition to improving operational reliability and encouraging a more sustainable and effective power management solution, these approaches provide the most flexible and affordable options, guaranteeing a smooth integration with our current system design.

Continuing our study, we have to create a power management system that, with fading noise models, improves the detection of power theft. Research by [33] and [34] shows that wireless and imaging systems commonly feature fading noise. Researchers can model its unique statistical features to detect abnormalities within power usage patterns. We propose detecting anomalies and illegal usage in the power networks by incorporating speckle noise models into advanced signal processing methods. This model improves the effectiveness and reliability of power theft detection methods. It cuts energy losses for utility companies by introducing a new method of highlighting subtle deviations that are difficult to notice with standard power monitoring systems. The research will also provide a flexible framework in grid systems that can be scalable and robust in various operational environments.

The smooth functionality of the power management system 'A Power Management Systems' in such a three-phase power scenario will ensure that similar systems will be better in robustness and flexibility. The implementation includes using advanced algorithms for adaptation to this three-phase setting; thus, it effectively enables dynamic load balancing by distributing single-phase loads over three phases to achieve a balanced set of loads through methods presented in [35]. Load stability and avoidance of the inherent inefficiencies of a phase imbalance are the twin demands of any three-phase system. Our design will enable the system to stabilize residential and industrial applications by efficiently mitigating neutral currents, thereby limiting power losses and preventing transformer overheating through techniques of optimal load redistribution, as suggested in [35]. By reducing operational losses and conserving energy, this improvement will better align with the goal of our study and support a more sustainable and effective power management solution. In a three-phase power situation, the system achieves excellent stability, prolongs the life of vital components, and utilizes energy much more efficiently.

Acknowledgement:
The authors wish to thank the University of Balamand for partial funding and for providing labs, equipment, and parts that were indispensable for the successful completion of this project. Additionally, they would like to extend special thanks to Mr. Hassan Ghannoum and Mr. Georges Semaan for their continuous support during the realization of the project. Their contributions to the project were tremendous and vital.

References:

[1] Geetha K. B., "Identification of Power Theft using Micro Controller" *International Journal of Trend in Scientific Research and Development (ijtsrd)*, vol. 2, no. 1, December 2017, pp. 1767-1772, URL: https://www.ijtsrd.com/papers/ijtsrd7134.pdf, Last Accessed February 24, 2025.

[2] A. Abdollahi, M. Dehghani, and N. Zamanzadeh, “SMS-based reconfigurable automatic meter reading system” in *Proceedings of the 16th IEEE International Conference on Control Applications, CCA 2007*, part of IEEE Multi-conference on Systems and Control, Singapore, 1-3 October 2007, pp. 1103–1107, doi: 10.1109/CCA.2007.4389381.

[3] H. Alalem, A. Fadel, A. Turki, M. Shlibek, and M. Shlibek, “Simulation of RF Technology Based Power Theft Detection” *European Journal of Engineering Science and Technology*, vol. 2, no. 1, 2019, pp. 95-105, doi: 10.33422/EJEST.2019.01.54

[4] S. N. Swami, A. B. Ghayal, H. G. Tamboli, and R. R. Suryawanshi, “Wireless Electricity Theft Detection by using ZIGBEE Technology” *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 5, no. 3, March 2016, pp. 1639–1643, doi: 10.15662/IJAREEIE.2016.0503097.

[5] C. L. Zulu and O. Dzobo, “Real-time power theft monitoring and detection system with double connected data capture system” *Electrical Engineering*, vol. 105, 2023, pp. 3065–3083, doi: 10.1007/s00202-023-01825-3.

[6] T. Malka, D. Sharma, and D. Singh, “A Survey of Monitoring and Controlling Power Theft Problem in Local Area” *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 3, no. 5, 2017, pp. 401–405, URL: https://www.ijariit.com/manuscripts/v3i5/V3I5-1263.pdf, Last Accessed February 24, 2025.

[7] A. Afridi, A. Wahab, S. Khan, W. Ullah, S. Khan, and S. Z. Ul Islam, “An efficient and improved model for power theft detection in Pakistan” *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 4, pp. 1828–1837, Aug. 2021, doi: 10.11591/eei.v10i4.3014.

[8] K. Blazakis and G. Stavrakakis, “Efficient Power Theft Detection for Residential Consumers Using Mean Shift Data Mining Knowledge Discovery Process” *Int. J. Artif. Intell. Appl.*, vol. 10, no. 1, January 2019, pp. 69–82, doi: 10.5121/ijaia.2019.10106.

[9] S. Chougule, M. Thite, A. Dalave, R. Nadaf, K. Randive, and S. Manjare, “GSM based electricity power theft detection” *Int. J. Innov. Eng. Res. Technol.* (IJIERT), vol. 7, no. 3, Mar. 2020, pp. 6–9, URL: https://repo.ijiert.org/index.php/ijiert/article/download/2074/1948/3896, Last Accessed February 24, 2025.

[10] S. Arivazhagan, T. A. Atiso, and M. A. Seid, “GSM and Arduino based power theft detection and protection” *Int. J. Adv. Res. Ideas Innov. Technol.* (IJIERT), vol. 5, no. 4, 2019, pp. 581–588, URL: https://www.ijariit.com/manuscripts/v5i4/V5I4-1363.pdf, Last Accessed February 24, 2025.

[11] C. Obasogie, S. W. Pallam, and I. M. Visa, “Automated electricity power theft identification and reporting system” *Int. J. Sci. Eng. Appl.*, vol. 12, no. 5, 2023, pp. 93–98, doi: 10.7753/IJSEA1205.1027.

[12] N. O. Shokoya and A. K. Raji, “Electricity theft mitigation in the Nigerian power sector” *Int. J. Eng. Technol.*, vol. 8, no. 4, 2019, pp. 467–472, doi: 10.14419/ijet.v8i4.29391.

[13] N. Mohite, R. Ranaware, and P. Kakade, “GSM Based Electricity Theft Detection” *Int. J. Sci. Eng. Appl. Sci.*, vol. 2, no. 2, Feb. 2016, pp. 445–449, URL: https://ijseas.com/volume2/v2i2/ijseas20160255.pdf, Last Accessed February 24, 2025.

[14] P. R. Malhotra and R. Seethalakshmi, “Automatic Meter Reading and Theft Control System by Using GSM” *Int. J. Eng. Technol.*, vol. 5, no. 2, Apr.–May 2013, pp. 806–810, URL: https://www.enggjournals.com/ijet/docs/IJET13-05-02-097.pdf, Last Accessed February 24, 2025.

[15] A. Kumar, D. Gupta, A. Jadon, A. Kumar, and J. Singh, “IoT power theft identification and monitoring” *Int. J. Eng. Adv. Technol.* (IJEAT), vol. 9, no. 5, June 2020, pp. 1100–1103, doi: 10.35940/ijeat.E1077.069520.

[16] P. Bhakta, S. Debnath, P. Debnath, P. Das, and S. Pal, “Power Theft Detection System” *Int. J. Creative Res. Thoughts* (IJCRT), vol. 10, no. 5, May 2022, pp. d631–d638, URL: https://www.ijcrt.org/papers/IJCRT2205409.pdf, Last Accessed February 24, 2025.

[17] R. Meenal, K. M. Kuruvilla, A. Denny, R. V. Jose, and R. Roy, “Power monitoring and theft detection system using IoT” in Proc. International Conference on Physics and Photonics Processes in Nano Sciences, Coimbatore, India, 2019, J. Phys.: Conf. Ser., vol. 1362, p. 012027, doi: 10.1088/1742-6596/1362/1/012027.

[18] G. L. Prashanthi and K. V. Prasad, “Wireless power meter monitoring with power theft detection and intimation system using GSM and Zigbee networks” *IOSR J. Electron. Commun. Eng.* (IOSR-JECE), vol. 9, no. 6, Nov.–Dec. 2014, pp. 4–8, doi: 10.9790/2834-09610408.

[19] A. Anand, R. Mukherjee, Y. Choudhary, and A. Yadav, “GSM Based Smart Energy Meter with Theft Detection and Load Control” in *Proc. 7th International Conference on Signal Processing and Communication* (ICSPC), Noida, India, Nov. 2021, pp. 59–62, doi: 10.1109/ICSC53193.2021.9673274.

[20] A. Jain, D. Kumar, and J. Kedia, “Design and development of GSM based energy meter” *Int. J. Comput. Appl.*, vol. 47, no. 12, June 2012, pp. 41–45, doi: 10.5120/7244-0302.

[21] R. P. Bhoge, J. Holey, V. Rajput, S. Rathod, Y. Raut, and P. Nandankar, “Leveraging IoT for detecting power and water theft in urban environments: A comprehensive review” *Int. J. Innov. Eng. Sci.*, vol. 9, no. 3, May 2024, pp. 60–68, doi: 10.46335/IJIES.2024.9.3.12.

[22] T. B. Smith, “Electricity theft: a comparative analysis,” *Energy Policy*, vol. 32, no. 18, 2004, pp. 2067–2076, doi: 10.1016/S0301-4215(03)00182-4.

[23] T. R. Memon, G. Murtaza, A. Basharat, K. Mahnoor, and F. Ali, “Automatic Power Factor Detection & Correction using Microcontroller” *J. Appl. Eng. Technol.*, vol. 2, no. 1, 2018, pp. 22–28, doi: 10.55447/jaet.02.01.44.

[24] A. Taye, “Design and simulation of automatic power factor correction for industry application” *Int. J. Eng. Technol. Manag. Res.*, vol. 5, no. 2, Feb. 2018, pp. 10–21, doi: 10.29121/ijetmr.v5.i2.2018.142.

[25] M. Madhiarasan, "Implementation of IoT-based energy monitoring and automatic power factor correction system" *Thermal Sci. Eng. Prog.*, vol. 6, no. 1, 2023, pp. 10–18, doi: 10.24294/tse.v6i1.1996.

[26] T. R. Wangchuk, N. T. Lepcha, B. Limbu, G. P. Siwakoti, A. Chettri, D. Lepcha, and P. Mangar, “Automatic Power Factor Correction Using Arduino” *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 12, no. 6, June 2024, pp. 1077–1080, doi: 10.22214/ijraset.2024.63268.

[27] R. A. Mahmoud, "Automatic power factor correction based on Pearson similarity for distribution networks" *The Journal of Engineering*, vol. 2022, pp. 798–831, 2022, doi: 10.1049/tje2.12162.

[28] R. A. Mahmoud and A. Emam, “Coherence-based automatic power factor correction (APFC) algorithm for power grids” *The*

Journal of Engineering, vol. 2022, no. 512, pp. 512–527, 2022, doi: 10.1049/tje2.12133.

[29] P. I. Udenze, T. K. Genger, and M. O. Ekoja, “An Arduino-Based Automatic Power Factor Correction Device” *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering* (IJIREEICE), vol. 7, no. 9, Sep. 2019, pp. 25–31, doi: 10.17148/IJIREEICE.2019.7905.

[30] A. G. Shende, S. W. Khubalkar, and P. Vaidya, "Hardware Implementation of Automatic Power Factor Correction Unit for Industry" in *Proc. AMSE 2021*, Nagpur, India, *J. Phys.: Conf. Ser.*, vol. 2089, 2021, p. 012032, doi: 10.1088/1742-6596/2089/1/012032.

[31] B. M. Rija, M. K. Hussain, and A. M. Vural, “Microcontroller-based automatic power factor correction for single-phase lagging and leading loads” *Engineering, Technology & Applied Science Research*, vol. 10, no. 6, 2020, pp. 6515–6520, doi: 10.48084/etasr.3916.

[32] P. V. Nandankar and P. V. Dhawas, “Automatic Power Factor Correction for Residential Consumers” *International Journal of Innovative Technology and Exploring Engineering* (IJITEE), vol. 9, no. 7, May 2020, pp. 574–578, doi: 10.35940/ijitee.G4937.059720.

[33] J. Dubois, “Segmentation of speckled ultrasound images based on a statistical model” in *Proc. 16th International Biosignal Conference* (EURASIP), Czech Republic, June 2002, pp. 377–380, URL: http://dx.doi.org/10.13140/RG.2.2.13945.79206, Last Accessed February 24, 2025.

[34] O. Abdul-Latif and J. Daba, “Supervised machine learning classifier for diversity combined signals in 6G massive MIMO receivers” *Universal Journal of Electrical and Electronic Engineering*, vol. 7, no. 6, 2020, pp. 320–327, doi: 10.13189/ujeee.2020.070604.

[35] M. El Hassan, M. B. El Najjar, and R. Tohme, “A Practical Way to Balance Single Phase Loads in a Three Phase System at Distribution and Unit Level” *Renewable Energy and Power Quality Journal* (RE&PQJ), vol. 21, July 2023, pp. 357–362, doi: 10.24084/repqj20.255

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Ali Chrakie and Moustapha El Hassan conceptualized the research.

Ali Chrakie, Moustapha El Hassan, and Jihad Daba developed the methodology.

Ali Chrakie simulated the proposed algorithm.

Ali Chrakie developed the online monitoring website.

Ali Chrakie and Moustapha El Hassan implemented the prototype and performed measurements.

Moustapha El Hassan and Jihad Daba carried out the validation.

Ali Chrakie, Moustapha El Hassan, and Jihad Daba conducted the formal analysis.

Moustapha El Hassan and Jihad Daba were responsible for the investigation.

Ali Chrakie provided the necessary resources and managed data maintenance.

Ali Chrakie and Moustapha El Hassan wrote the initial draft.

Ali Chrakie, Moustapha El Hassan, and Jihad Daba reviewed and edited the manuscript.

Ali Chrakie and Moustapha El Hassan prepared the visualizations.

Moustapha El Hassan was responsible for supervision.

Ali Chrakie and Moustapha El Hassan managed the project.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

The University of Balamand funded this study.

Conflict of Interest

The authors have no conflicts of interest to declare.